

Common Security Requirements Language for Procurements & Maintenance Contracts PCSF, June 7, 2006 La Jolla, CA

Rita Well, Idaho National Laboratory

Control Systems Security Program

National Cyber Security Division



Homeland
Security

The SCADA/Control System Security Project:

Common Security Requirement Language for Procurements & Maintenance Contracts

<http://www.cscic.state.ny.us/msisac/scada/>

Will Pelgrin, New York State

Michael Assante, Idaho National Laboratory

Rita Wells, Idaho National Laboratory



Homeland
Security

Control System Security Project

Providing owner & operators more secure systems...



...to manage the risk & head off tomorrow's legacy problem

- Asset owner driven with participation from all stakeholders (100+ team members)
- Launched at the SANS SCADA Summit in Orlando in March
- Will provide a specific deliverable to buyers & operators ("Asset Owners")
 - Common security requirement language for procurements & maintenance contracts
 - Designed as a "Tool Kit" or desk reference



Homeland
Security

Project Goal & Scope

The Goal

Develop common procurement requirements and contractual language that the owners can use to ensure control systems they are buying or maintaining that have the best available security

Scope of the project

**New control systems
Maintenance of systems
Legacy systems
Information and personnel security**

SCADA Procurement Objectives

Deliverables:

Identify the working group 

Create a timeline with deliverables 

SCADA Procurement Objectives (Cont.)

Deliverables:

Phase One

Develop a straw Document

Identify Critical Components (opportunities for immediate progress)

Publish Security Specification for Key Components of Control Systems Including but not Limited to:

- **Lock down services**
- **Patch management services**
- **Vulnerability scans**
- **Code reviews**

SCADA Procurement Objectives (Cont.)

Deliverables:

Phase Two

Develop a Complete Comprehensive Document of Procurement and Contractual Language

Identify all Aspects of Control Systems

Develop Specifications Requirements

SCADA Procurement Objectives (Cont.)

Deliverables:

Create Secure Website for Publishing Deliverables

Done – <http://www.cscic.state.ny.us/msisac/scada/>

Develop a procurement and Maintenance desk reference

– DRAFT is in progress and will be posted soon

Solicit State and Local Governments

Identify which Entities which will Participate in an

Aggregate Procurement

SCADA Procurement Objectives (Cont.)

Guiding Principles:

Collaboration

Everyone at the table

Owners, regulators, vendors

Win-Win

Risk Reduction

Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks

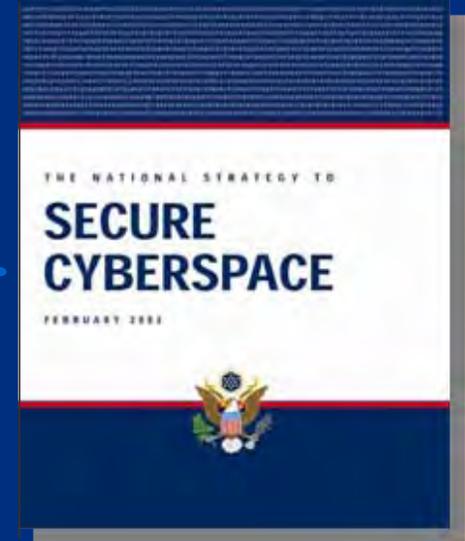
Software Assurance

A Strategic Initiative to Promote Integrity, Security, and Reliability in Software

Procurement Specification for Control Systems

Initiative to develop procurement language for control systems (hardware and software)

March 16, 2005



Hun Kim

Deputy Director for Strategic Initiatives
National Cyber Security Division
US Department of Homeland Security



Homeland
Security



Control Systems Security Program

Reduce control systems security risk across all of the critical infrastructure sectors

- DHS funding for the project
- Working with vendors
- Participated in standards and practice development
- Focused on providing valuable tools to Asset Owners to manage control system security risk



Homeland
Security



DOE National SCADA Test Bed

Reduce energy infrastructure security risk through asset owners and technology providers & work to the roadmap

- Control systems security testing
- Working with vendors
- Develop a body of common vulnerabilities and technology risks
- Testing engineers work with asset owners and vendors
- The DOE program has already resulted in enhanced systems



The Time is Right for this Action



Control Systems Procurement Cycle

	Request for Proposal	Proposal Submittal	Bid Review	Contract Award	Statement of Work (SOW)	Design Review	Document Review	Factory Acceptance Test (FAT)	Site Acceptance Test (SAT)
<i>Asset Owner</i>	X		X	X	X	X	X	X	X
<i>Consultant</i>	X		X		X			*	*
<i>Vendor</i>		X		X	X	X	X	X	X

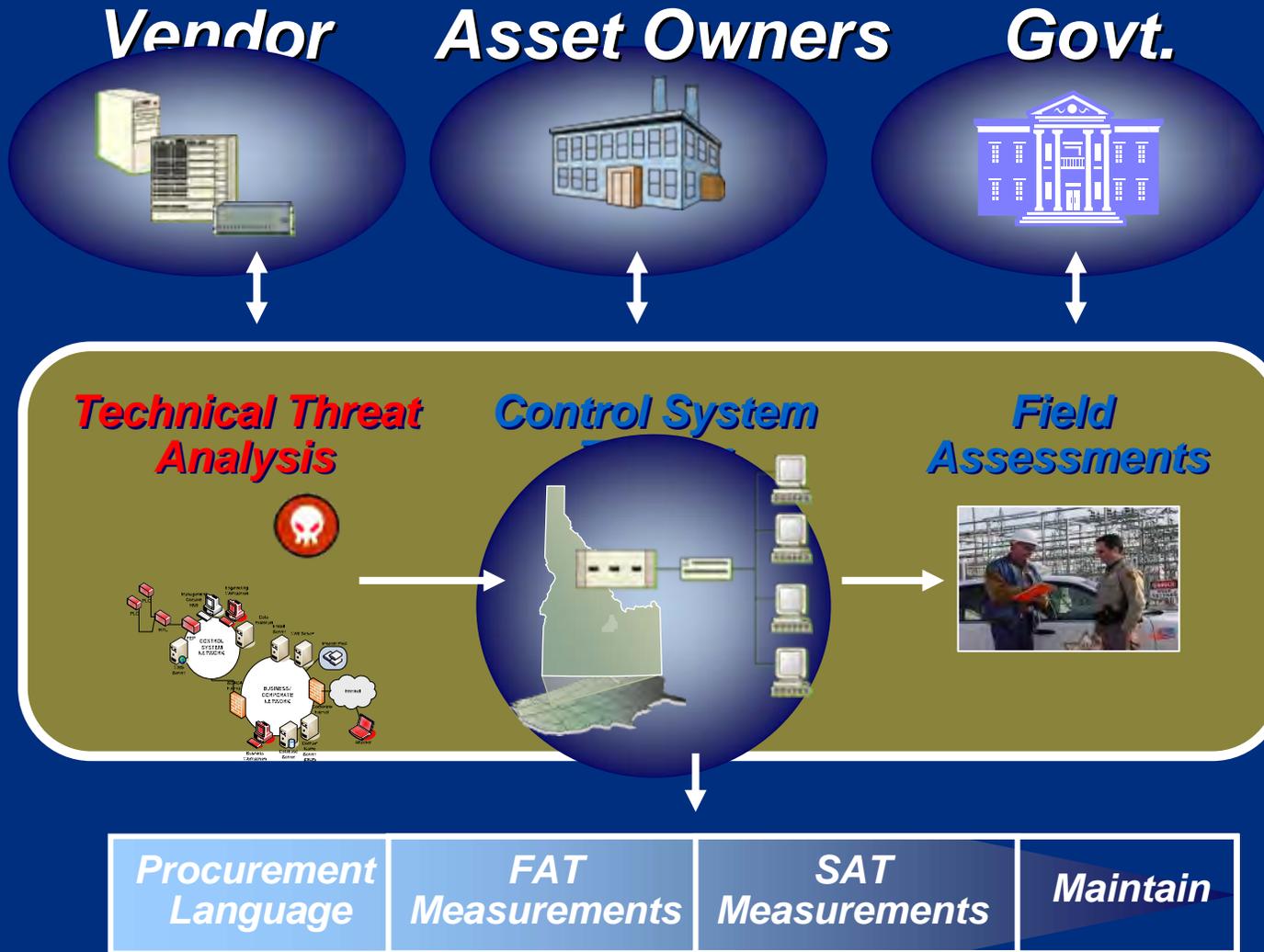
* Occasionally participate

<i>Procurement Language</i>	<i>FAT Measurements</i>	<i>SAT Measurements</i>	<i>Maintain</i>
-----------------------------	-------------------------	-------------------------	-----------------



Homeland Security

Working Together to Deliver & Operate Secure Systems



Homeland Security

Procurement Language

- Aggressive project designed to provide a “buyers” tool kit
- Provide security requirements for inclusion into RFPs
- Use common, grounded and valuable language
- Support Bid Reviews (gauge responsiveness)
- Provide the detailed required to support SOW development and Design Creation & Review
- Starting with greatest risk that can be addressed



Factory Acceptance Test Measurements

- Linked to the procurement requirement
- Provides language to include in Factory Acceptance Testing requirements and specifications
- Designed to validate the requirement has been met



Site Acceptance Test Measurements

- Linked to the procurement requirement
- Provides language to include in Site Acceptance Testing requirements and specifications
- Designed to validate the risk reducing requirement is not lost during implementation in the Asset Owners environment
- Important step that requires an understanding of “why it was delivered that way”
- First hand-off from the procurement / provider team to the actual operator and maintainer

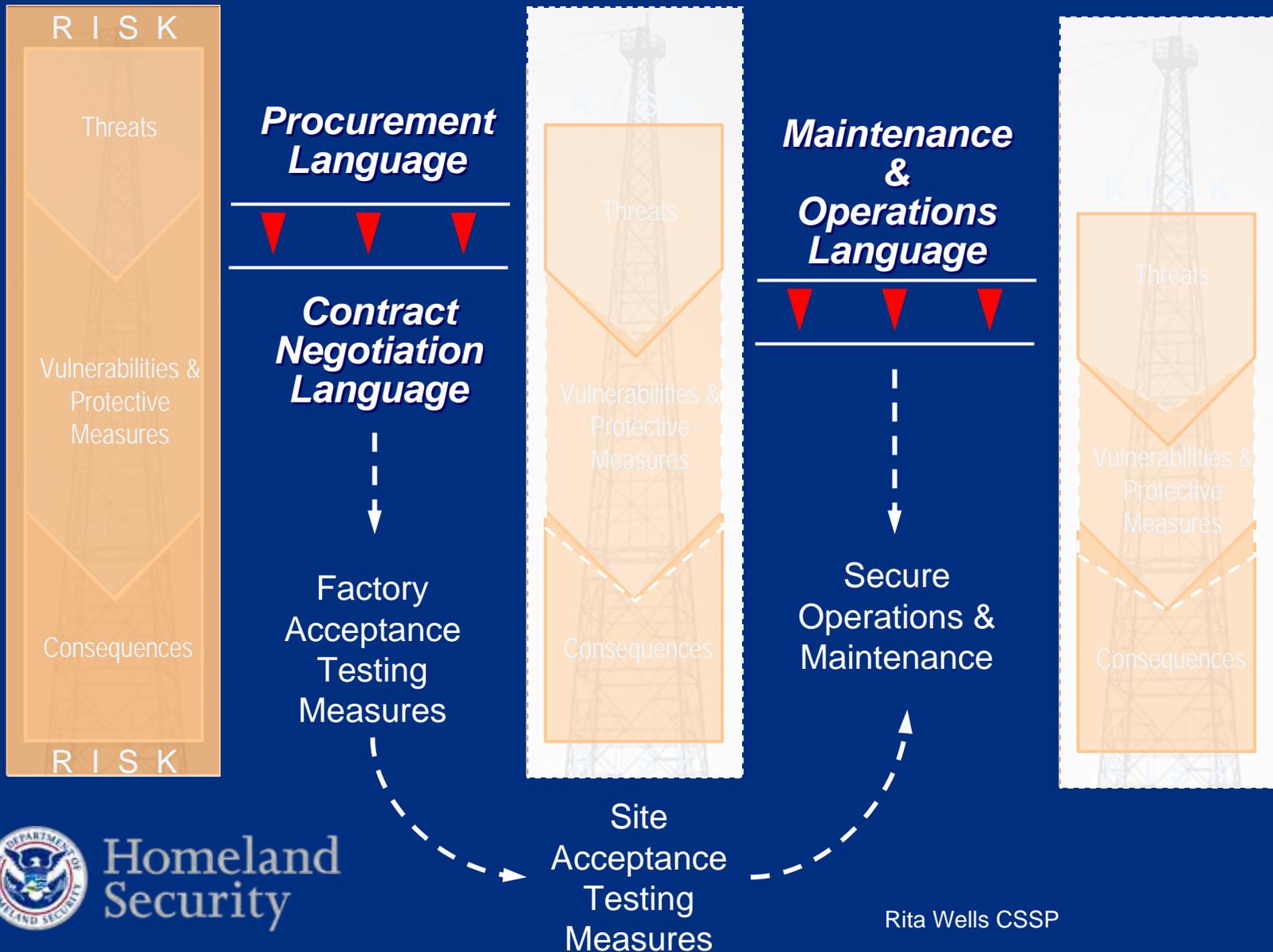


Maintenance Language & Operating Guidance

- Linked to the procurement requirement
- Provides language to include in maintenance contracts
- Designed to further reduce the risk to control systems during their life-time
- Critical step to ensure the benefits of the security requirements are not lost during the technologies operational lifespan
- Requires an understanding of “why it was delivered that way”



Project Risk Reduction Scheme



Project Scope

Driving for a Phase-I deliverable engineered to provide immediate value for asset owners

Phase I Scope

Technology

- Control system network-level
- Control center systems
 - SCADA/EMS
 - Management
 - Plant control
- Networked communications

Security

- High value opportunities
 - Greatest risk reduction
 - Most consensus and knowledge
- Compliance driven requirements
 - Initial industry guidelines
 - Some standards

Industry

- All industries that employ control systems
- Industry applicability and value will be driven by the technology/security scoping elements

Phase II – Possible Future Scope

Technology

- Devices in the field/plant floor
 - IEDS, PLC, RTU, Controllers
- Safety systems
- Remote systems
- Serial communications
- Wireless

Security

- More comprehensive security requirements
- Security for specialized technologies
- Expand industry guidance and standards being incorporated

Industry

- Focus on expanding to meet more specialized application of control system technology
- Expand the value and specificity for all industries

Security Areas To Be Covered

- Clear text communications
- Account management
- Authentication
- Coding practices
- Unused services
- Network addressing
- System integration
- Unpatched components
- Web services
- Perimeter protection
- Human/personnel controls

Proposed Categories

- System Hardening
- Perimeter Protection
- Account Management
- Coding Practices
- Flaw Remediation
- Network Partitioning
- Dynamic Addressing
- Antivirus Management
- Remote Access

Proposed Future Categories

- Availability
- Integrity
- Confidentiality
- Policies and Procedures
- Configuration Management
- Recovery and Backup
- Disaster Recovery
- Wireless
- Lifecycle Issues
- System Integration
- Logging and Auditing
- Training
- Least Privilege
- Enumeration
- Physical Access
- Contract Services
- Redundancy

A Page From the Tool Kit

- Procurement Topic
- Basis Security Risk
- Procurement Language
- Language Guidance
- FAT Measurements
- SAT Measurements
- Maintenance Guidance
- References

DRAFT Example from System Hardening DRAFT

Topic: *Installing OS and software updates*

Basis: Most successful cyber attacks occur in unpatched systems or applications. Patches and software updates, including anti-virus scanners, are required to lessen the possibility of cyber attack upon known vulnerabilities and exploits. Software updates should be applied to the operating system, vendor provided applications, communications drivers, and/or firmware.

Procurement Language: The vendor shall provide notification of a known vulnerability effecting vendor supplied or required software within a negotiated period of time after public discloser, and appropriate software updates and/or workarounds to mitigate the vulnerability within a negotiated period of time shall be provided. The vendor shall provide passive scanning capabilities.

Language Guidance: Most networked services have been the target of a number of attacks over the years...



DRAFT Example from System Hardening (cont)

Topic: Installing OS and software updates (cont)

Language Guidance: ... Responsible system and product vendors regularly release updates, patches, service packs or other fixes to their products to address known and potential vulnerabilities. Of course, to be effective, these must be installed...
Active scanning of control system networks have been known to disable the networks during operations. FAT and SAT provide opportunities to active scanning without an impact to production. Even passive scanning is not recommended on production systems until the impact is fully understood to operations. Scanning is an effective tool for to be used on non-production systems to identify vulnerabilities.

FAT Measures: The vendor shall at the start of FAT update current patches. The vendor shall as part of FAT perform virus scans to ensure that the system has not been compromised during the testing phase.

SAT Measures: The vendor shall at the start of SAT update again current patches. The vendor shall as part of SAT perform virus scans to ensure that the system has not been compromised during the testing phase.

Maintenance Guidance: The purchaser shall negotiate with the vendor, a patch management process to include policies and procedure for the system after installation. It is in the purchasers best interest to make the provisions part of the procurement language.

References: CIP-007-1 R3



Homeland
Security

DRAFT

Removal of services and programs not required for control system operation and maintenance

Basis: *Unused services in a Host operating system (OS) that are left enabled are possible entry points for exploits on the network and are generally not monitored since they are not used. Only the services used for control systems (CS) operation and maintenance should be enabled.*

Procurement Language: *The vendor shall provide documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and their appropriate configuration, including revisions and/or patch levels for each of the computer systems associated with the control system. A listing of services required for any computer system running control system applications or required to interface to control system applications will also be provided by the vendor. All services shall be patched to current status.*



DRAFT Example System Hardening (Cont.) DRAFT

Topic: Removal of Services (Cont)

FAT Measures:

The purchaser requires that the results of assessment scans (as a minimum a vulnerability and active port scan) run on the system, as a primary activity of the FAT, be compared with an inventory of the required services and their patching status, in addition to verification of the required documentation, to validate this requirement. Other measures include:

For each networked device or class of device (e.g. server, workstation, switch), provide the following configuration documentation: A listing of network services required for operation of that device. Indicate service name, protocol (e.g. TCP, UDP) and port range. A listing of dependencies on underlying Operating System services. A listing of dependencies on networked services residing on other devices. A listing of the all software configuration parameters required for proper system operation. A listing of certified operating system, driver and other software versions installed on the device. A list of results found by the vulnerability scans with mitigations effected. Install firmware updates available for the computer or device certified by the system manufacturer at the time of installation.

Provide a summary table indicating each communication path required by the system. Include the following information in this table: Source device name and MAC/IP address.

Destination device name and MAC/IP address. Protocol (e.g. TCP, UDP) and port.

Perform network-based validation and documentation steps on each device: Perform a full TCP and UDP port scan on ports 1-65535. This scanning needs to be completed during 'normal system operation.

DRAFT Example from Perimeter Protection DRAFT

Topic: *Canary*

Basis: Due to the fact that many control networks contain proprietary protocols, traffic signatures which would allow the use of a commercial NIDS do not exist. A honey pot (which analyzes unauthorized connections) or canarys (which simply indicate a connection attempt has taken place) have been implemented in certain configurations to provide passive network monitoring.

Procurement Language: For vendors that supply a canary, they shall supply it with a HIDS and alerting software to indicate connections.

Language Guidance: Canarys only work in a static address topology or where dynamic host control protocol (DHCP) is not used. It is recommended that retaliatory devices/actions (poison boxes) not be used.

FAT Measures: The canary should be installed and tested during the FAT if supplied by the vendor. Procedures should include accessing the device to demonstrate it detects connection attempts and alerts appropriately.

SAT Measures: The canary should be installed and tested during the SAT.
Maintenance Guidance: Changing network address topologies can require canaries to be reconfigured.

References: CIP-005-1 R2



DRAFT Example from System Hardening DRAFT

Topic: Communications Health Signals

Basis: *Communications Health (also known as Heartbeat signals, Health status) or protocols can be corrupted, spoofed, or possibly used as an entry point for unauthorized access.*

Procurement Language: *Heartbeat signals or protocols must be identified as to whether they should be included in network monitoring. The vendor shall provide packet definitions of the heartbeat signal if applicable. The vendor shall provide an example of the heartbeat traffic.*

Language Guidance: *Heartbeat status signals can be sent over serial connections or routed protocols. They indicate communications health of the system. These are often used in reporting-by-exception schemes, and may be used by third party add-on applications.*

FAT Measures: *FAT procedures should include validation and documentation of this requirement. The vendor shall create a baseline of the heartbeat traffic.*

SAT Measures: *SAT procedures should include validation and documentation of this requirement. The vendor shall create a baseline of the heartbeat traffic.*

Maintenance Guidance: *The frequency of the heartbeat is normally configurable. If changed, the network monitoring will need to be modified.*

References: *CIP-005-1 R1*



Join the Project!

Thank You

Will Pelgrin – william.pelgrin@cscic.state.ny.us

Michael Assante – Michael.Assante@inl.gov

Rita Wells – Rita.Wells@inl.gov

Project Web Site:

<http://www.cscic.state.ny.us/msisac/scada/>



Homeland
Security



Homeland Security